METHODS AND APPARATUS FOR
IMPLEMENTING A CRYPTOGRAPHY ENGINE

Abstract of the Disclosure

Methods and apparatus are provided for implementing a cryptography engine for cryptography processing. A variety of techniques are described. A cryptography engine such as a DES engine can be decoupled from surrounding logic by using asynchronous buffers. Bit-sliced design can be implemented by moving expansion and permutation logic out of the timing critical data path. An XOR function can be decomposed into functions that can be implemented more efficiently. A two-level multiplexer can be used to preserve a clock cycle during cryptography processing. Key scheduling can be pipelined to allow efficient round key generation.